January 2015

Michigan Cyber Initiative Newsletter

Articles of Interest

Former Chairman Mike Rogers Warns of Cyber Attacks

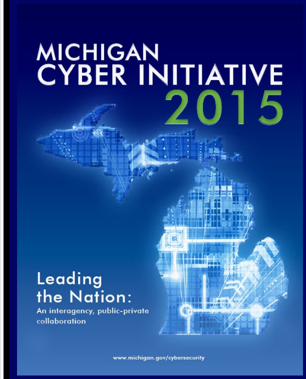
Rogers points out the need for information-sharing legislation. He warns that something should be done soon and that information sharing can assist in defending against cyber attacks. (Read more here.)

Cyber Marines

The Marines recently demonstrated cyber war on the battlefield using various technologies. (Read more here.)

FedRamp Roadmap

The General Services Administration has issued a two-year roadmap aimed at improving and enhancing the FedRamp initiative. The initiative will allow the vetting process to take place more quickly and with fewer hurdles. (Read more here.)


MICHIGAN
CYBER INITIATIVE
2015
Leading the Nation:
An interagency, public-private collaboration
www.michigan.gov/cybersecurity

Michigan's 2015 Cyber Initiative

Michigan continues efforts to protect and defend our most valuable assets through education and awareness, economic development and collaboration. (Click on the picture for more.)

Michigan Cyber Initiative News offers updates on Governor Rick Snyder's cyber initiative as well as knowledge and awareness on cybersecurity issues. This monthly newsletter is produced by the Michigan Department of Technology, Management and Budget - Office of Cybersecurity.

CySAFE

In the world of cybersecurity, local governments often struggle to keep pace with an ever-changing threat environment. Small and mid-sized agencies can take advantage of CySAFE, a free IT security assessment tool that helps them assess, understand and prioritize their basic security needs.

CySAFE was developed collaboratively by Livingston, Monroe, Oakland, Washtenaw and Wayne counties and the State of Michigan. Developers relied on three well-known IT security Frameworks — SANS top 20 critical controls, ISO 27001 and NIST. The goal was to combine controls from all three frameworks into one master list, remove redundant controls and assess the controls against the agency's current IT security capabilities. Adopting these standards, rather than creating new ones, took advantage of the work that was already done, built on a common language for security measures, provided a benchmark for comparison of readiness across organizations and supported needed investments in IT security capabilities.

Agencies are encouraged to use tools such as CySAFE to safeguard their information.

"It is our responsibility to be good stewards of public data," said David Behen, director of the Department of Technology, Management and Budget and Michigan's chief information officer. "Working with our partners at the state and local levels will make us all better at recognizing and eliminating cyber threats in an ever-changing environment."

CySAFE is free to all government agencies through the G2G Marketplace. An initial assessment, which takes an hour to complete, provides a prioritized listing of IT security gaps and offers an iterative graphing feature to mark progress. Since its rollout in September 2014, the CySAFE tool has been downloaded nearly 200 times by local governments nationwide.

To obtain a free copy of CySAFE, follow these easy steps:

1. Go to www.g2gmarket.com
2. Register with the G2G Marketplace
3. Download your free copy

Improve Your Cyber Security Posture

With the holiday season behind us, there is an even larger supply of computers, laptops, tablets and other connected devices that are vulnerable to attack and exploitation. During this time of the year, many of us made New Year's resolutions to lose weight, pay off debt, and be more physically and mentally fit. The list goes on and on. But in the haste of this new year, perhaps an additional resolution would be to increase your personal cybersecurity posture and awareness.

Why increase your personnel cybersecurity posture and awareness? This question was answered in 1735 by Benjamin Franklin as he wrote in the Pennsylvania Gazette, "An ounce of prevention is worth a pound of cure."

Over the past 24 months, countries around the world, including the United States, have witnessed an ever-increasing number of cyber attacks. More than likely, this trend is not going to stop any time soon. With this in mind, why not take some basic steps to increase your cyber security and awareness posture at home and at work?

How can you do this? There are a multitude of resources available. Let's start with the basics as identified by the United States Computer Emergency Readiness Team (US-CERT). US-CERT offers 12 actions home users can take to protect their computer systems. Take a few moments this new year to review these actions and instill additional rigor into your day-to-day activities. Here are some of the basics in no particular order.

1. Use virus protection software and keep it up to date.
2. Keep all applications, including your operating systems, patched.
3. Don't open unknown email attachments.
4. Turn off your computer or disconnect from the network when not in use.
5. Make regular backups of critical data.

It is important to realize that we can't protect ourselves from every vulnerability and attack. As with the human body, people who practice good preventative care are more likely to have fewer health problems. Many of us take vitamins or work out to stay healthy. Instill this similar habit into your cyber activities. Practice and start doing the basics: don't share passwords, change your passwords on a regular basis, avoid public hot spots, utilize virus protection, and keep your operating systems and software up to date. Practice the good security habits that are recommended at https://www.us-cert.gov/ncas/tips/ST04-003.

In addition to US-Cert, the Federal Bureau of Investigation (FBI) discusses How to Protect Your Computer using the same advice parents might deliver to young drivers on their first solo journey. These guidelines apply to everyone who wants to navigate safely online. A special agent in our Cyber Division suggested, "Don't drive in bad neighborhoods. If you don't lock your car, it's vulnerable. If you don't secure your computer, it's vulnerable. Reduce your vulnerability, and you reduce the threat."

How much information do you openly share on the Internet? In addition to the physical domain, it is important to practice good social networking habits. Take a moment and Google yourself. How much information is out there? Consider how much of this information you really want available to everyone in the world. How many "friends" on social media sites do you have that you actually know and trust? Be cautious about the amount of personal information you share across your social media accounts. The more information you have out there, the easier you are to target. Many often say it is not a matter of *if.* It is more a matter of *when.* Why not take a moment to be proactive and challenge this sentiment? Don't be the easy target online.

Like other New Year's resolutions, some become reality while others drift to the wayside. Take the challenge to be proactive and increase your personal cybersecurity posture and awareness. Add this resolution to your list of things to do, take the initial steps and help prove a 200-year-old saying that "an ounce of prevention is worth a pound of cure" — even as it relates to the ever-changing and evolving cyber domain.

Author: Major Daniel Guy, Commander, 110th Communications Flight, Michigan Air National Guard